UNCLASSIFIED

Desktop Applications General

Version: 4

Release: 1

03 Dec 2009

STIG.DOD.MIL

Sort Order: Group ID (Vulid), ascending order
Notice: Developed by DISA for the DoD
Description:

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System= SECRET Checklist
Top Secret System = SECRET Checklist

Group ID (Vulid): V-6355
Group Title: DTGW001-Appropriate backup strategy does not exist
Rule ID: SV-6428r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTGW001
Rule Title: An appropriate backup strategy does not exist for the data.

Vulnerability Discussion: Data integrity and availability are key security objectives. Adequate data backup is one strategy that is crucial to meeting these objectives. Although users of desktop applications may not be creating mission critical data, all their data represents a resource that, if lost, could result in a permanent loss of information or productivity.

A backup strategy is highly dependent on the physical and logical environments. In environments where users frequently operate disconnected from a LAN, as in the case of notebook PC users who travel, it is not generally practical for the users to store all their data on a file server. Developers may require standalone copies of program code while additions or alterations are in progress. For these and other reasons, strict requirements for desktop backup are not addressed in this document. However, this section does provide recommendations that should be considered.

Users should make conscious decisions about the physical location where desktop application data is stored. They should be aware of the backup policy for that location. Any backup policy should be implemented in accordance with the following:

- Mission critical data should be stored on file servers with a formal data backup policy. Storage of mission critical data on desktop machines should be considered temporary.

- To the greatest extent possible, data files should be stored in a directory hierarchy that is separate from program files.

- An incremental, or change-based, backup solution can be used daily.

- A full data backup solution should be used at least weekly.

- Use of a Compact Disk-Recordable (CD-R) or Compact Disk-ReWritable (CD-RW) drive should be considered for desktop machines. CD-R and CD-RW disks provide high capacity at relatively low cost.

- The backup data should be stored on media or another machine that is not physically close to the original data source.

- Backup media should receive proper care according to its characteristics. Regular rotation of tape media is necessary to ensure usability. The media should be clearly labeled, including any appropriate security classification marking.

- Backup tools and schedules should be documented.

- Restoration tools and methods should be documented and they should be tested via restoration at least annually.

Responsibility: System Administrator

Check Content:
Procedure: Interview the SA to determine the type of data being housed on the machine. Interview the SA to determine the backup process being used for the data.

Criteria: If there is no backup process or the backup process is inadequate for the data on the machine, this is a finding.

Fix Text: Interview the SA to determine the type of data on the machine and its backup process. If there is no backup process or the process is inadequate, have the SA create a new backup process.

Group ID (Vulid): V-6356
Group Title: DTGW002-Public instant message clients are install
Rule ID: SV-6429r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTGW002
Rule Title: Public instant message clients are installed.

Vulnerability Discussion: Instant Messaging or IM clients provide a way for a user to send a message to one or more other users in real time. Additional capabilities may include file transfer and support for distributed game playing. Communication between clients and associated directory services are managed through messaging servers. Commercial IM clients include AOL Instant Messenger (AIM), MSN Messenger, and Yahoo! Messenger, and Skype. The Windows XP operating system includes the Windows Messenger component as an IM client. (This should not be confused with Windows Messaging which is a service within Windows.)

IM clients present a security issue when the clients route messages through public servers. The obvious implication is that potentially sensitive information could be intercepted or altered in the course of transmission. This same issue is associated with the use of public e-mail servers.

In order to reduce the potential for disclosure of sensitive Government information and to ensure the validity of official government information, IM clients that connect to public instant messaging services will not be installed.

NOTE: Clients used to access an internal or DoD controlled IM applications are permitted.

Responsibility: System Administrator

Check Content:
Procedure: Using Windows explorer search for the following files:
ymsgr*.exe, aim.exe

Criteria: If any of the files are found, this is a finding.
Note: If the file is tied to an IM application that is DOD controlled, this is not a finding.

Fix Text: Use Windows explorer to search for the files ymsgr*.exe and aim.exe. If found, delete them unless the file is tied to an IM application that is DoD controlled.

Group ID (Vulid): V-6357
Group Title: DTGW003-Peer to Peer clients or utilities are inst
Rule ID: SV-6430r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTGW003
Rule Title: Peer to Peer clients or utilities are installed.

Vulnerability Discussion: File-sharing utilities and clients can provide the ability to share files with other users (Peer-to-Peer Sharing). This type of utility is a security risk due to the potential risk of loss of sensitive data and the broadcast of the existence of a computer to others. There are also many legal issues associated with these types of utilities including copyright infringement and intellectual property issues. These types of utilities and clients include the following examples, Napster, Gnutella, Kazaa, and Freenet.

NOTE: Clients used to access an internal or DoD controlled file-sharing system are permitted.

Responsibility: System Administrator

Check Content:
Procedure: Using Windows explorer search for the following files:
napv.exe, Gnutella.exe

Criteria: If any of the files are found examine it to determine if it is a file sharing utility. If it is, this is a finding.

Fix Text: Use Windows explorer to search for the files *napv.exe and Gnutella.exe. If found and they are determined to be a file sharing utility, delete them.

Group ID (Vulid): V-6878
Group Title: DTGW004-Execution Restricted File Type Properties
Rule ID: SV-7145r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTGW004
Rule Title: Execution Restricted File Type Properties

Vulnerability Discussion: For certain file types, it is necessary to take steps to ensure that the default method of opening the file does not allow mobile code to be executed. Two techniques to achieve this goal are discussed here—altering the default file type Action and deleting the file type definition. Although methods of removing Microsoft's Windows Script Host (WSH) component might meet most of this requirement, that technique should not be the first choice. It would disable functionality that might be in use for other purposes, and the specific method used would have to be compatible with the Windows File Protection (WFP) feature present in later versions of Windows.

The default Action property can be altered to change the standard default Action from Open to Edit. When this technique is used, instead of executing a program with the file contents as code, an editor is opened with the file contents as a document. For example for a .vbs file, the Open action may be the command 'C:\WINNT\System32\Wscript.exe "%1" %*' and the Edit action may be the command 'C:\WINNT\System32\Notepad.exe "%1" %*'. Changing the default action to Edit results in a Notepad window opening up instead of the file being executed by the Windows Scripting Host when the .vbs file is opened. For non-technical user communities, an alternative that may be more appropriate is to have the Edit action be the command 'C:\WINNT\System32\Notepad.exe "C:\MC_Warn.txt"', where the file C:\MC_Warn.txt is created locally and contains a warning that the user has attempted to open a potentially dangerous file.

When altering the default file type Action is the technique used, the Always show extension setting adds additional value. This ensures that users can see the file type before attempting to open it.

While the alternate technique of deleting existing Windows file type definitions does provide security, it is not always a more secure long-term solution. During maintenance or product installation, a non-existent file type is usually defined while existing file type properties are usually not overwritten.

Regardless of which technique is used, the significant result is that when an attempt is made to open certain files using default application actions, any code in the file is not executed.

FIle extensions of certain files should not be hidden. Users can double click a file without knowing what type of file (or which application) is being opened.

Responsibility: System Administrator

Check Content:
Start the Windows Explorer application. On the Tools menu, select the Folder Options… item. On the Folder Options window, select the File Types tab. For each of the file types in the table below, select the Edit… button for Windows NT or the Advanced button for Windows 2000/2003/XP.

a) Determine the default Action by looking in the Actions: list for an action in bold font. A typical default action is indicated as "Open". If none of the entries in the Actions: list appears in bold font, the "Open" action is the default Action. Select the default Action and the Edit… button to determine the application used to perform the action.
b) Determine the value of the Always show extension option.

File Type	Extensions	File Type	Extensions
JScript Script File	JS	Windows Script Component	SCT,WSC
JScript Encoded Script File	JSE	Windows Script File	WSF
Scrap object	SHS,SHB	Windows Script Host Settings File	WSH
HTML Applications as Mobile Code	HTA		
VBScript Encoded Script File	VBE		
VBScript Script File	VBS		

NOTE: The File Type strings (e.g., "JScript Script File") may vary according to the specific software release. The key element for the check is the Extension value.

Criteria: If a file type is not defined, this is not a Finding.
a) If the application defined to perform the default Action could execute code in the file, then this is a Finding. For example, if the default Action for file type .VBS specifies wscript.exe as the application, a Finding is indicated. On the other hand, if the default Action for any file type specifies notepad.exe as the application, there is not a Finding.
b) If the Always show extension option is not enabled for each file type, then this is a Finding.

For Windows Vista open the Control Panel select Default Programs select Associate a file type or protocol with a Program:

a) Determine the default program by looking in the Current Default: list. A typical default action is indicated as "Open". If none of the entries in the Actions: list appears in bold font, the "Open" action is the default Action. Select the default Action and the Edit… button to determine the application used to perform the action.
b) Determine the value of the Always show extension option.

File Type	Extensions	File Type	Extensions
JScript Script File	JS	Windows Script Component	SCT,WSC
JScript Encoded Script File	JSE	Windows Script File	WSF
Scrap object	SHS,SHB	Windows Script Host Settings File	WSH
HTML Applications as Mobile Code	HTA		
VBScript Encoded Script File	VBE		

VBScript Script File	VBS

NOTE: The File Type strings (e.g., “JScript Script File”) may vary according to the specific software release. The key element for the check is the Extension value.

Criteria: If a file type is not defined, this is not a Finding.
a) If the application defined in the Current Default list could execute code in the file, then this is a Finding. For example, if the default program for file type .VBS specifies wscript.exe as the application, a Finding is indicated. On the other hand, if the default Action for any file type specifies notepad.exe as the application, there is not a Finding.

Fix Text: Change the default action to an application that will not execute the file such as notepad.exe and ensure that the Always show extension is enabled for the filetype in question.

Group ID (Vulid): V-6879
Group Title: DTGW005-Open_restricted File Type Properties
Rule ID: SV-7146r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTGW005
Rule Title: Open-restricted File Type Properties

Vulnerability Discussion: For some file types, providing the user an opportunity to cancel the opening of the file provides adequate protection for most environments. Files that are opened with applications that include internal controls on code execution are good candidates for this technique.

The Open Confirmation property, enabled through the Confirm open after download setting, provides a notice to the user that allows them to open the file, save the file to disk, or cancel the file open task. The Always show extension setting adds additional value. This ensures that users can see the file type before attempting to open it.

The Values of confirm after download and always show extension give the users additional information about a file so a decision can be made as to whether it should be opened.

The command line tool, ’assoc’, can be used to determine if a given file type definition exists. For example, on typical Windows systems the command ’assoc.bat’ returns ’.bat=batfile’ indicating that the extension .bat is defined and that the properties are stored in the Windows Registry under the key batfile.

Windows Explorer can be used to manually display and configure the Actions, Always Show Extension, and Open Confirmation properties. In Windows 2000 and XP use the File Types tab of the Tools | Folder Options dialog in Windows Explorer.

It must be recognized that performing these changes does not eliminate the danger from malicious code. Such code could come from a number of sources and use trigger techniques other than the Windows file type open action. Thus the changes documented here are not a substitute for an anti-virus tool with current definitions.

NOTE: The application of this change affects the behavior of all Windows applications that utilize the affected Registry settings.

Responsibility: System Administrator

Check Content:
Start the Windows Explorer application. On the Tools menu, select the Folder Options… item. On the Folder Options window, select the File Types tab. For each of the file types in the table below, select the Edit… button for Windows NT or the Advanced button for Windows 2000/2003/XP. On the Edit File Type window:

a) Determine the value of the Confirm open after download option.
b) Determine the value of the Always show extension option.

File Type	Extensions	File Type	Extensions
Adobe Acrobat Document	PDF	Microsoft PowerPoint Presentation	PPT
Adobe Acrobat Forms Document	FDF,XFDF	Microsoft PowerPoint Slide Show	PPS
LotusScript Library	LSL	Microsoft PowerPoint Template	POT
LotusScript Object	LSO	Microsoft Word Backup Document	WBK
Jscript	JS,JSE	HTML Applications	HTA
LotusScript Source	LSS	Microsoft Word Document	DOC
Microsoft Excel Backup File	XLK	Microsoft Word Template	DOT
Microsoft Excel OLE DB Query Files	RQY	MS-DOS Batch File	BAT
Microsoft Excel Web Query File	IQY	PostScript	PS,EPS
Microsoft Excel Template	XLT	Rich Text Format	RTF
Microsoft Excel Worksheet	XLS,XLB	WordPerfect Coach	WCH
VISIO	VSS,VST,VSD,VSW	Microsoft Access	AD, ADP,MDB,MDE
Shockwave	DCR,DXR,DIR,SPL, SWF	Flash	FLS
Shell Scrap Object	SHS, SHB	WordPerfect Macro	WCM
Windows Script Component	WSC, SCT		
Windows Script File	WSF		
Windows Script Host Settings File	WSH		
VBScript	VBE, VBS		

NOTE: The File Type strings (e.g., “LotusScript Library”) may vary according to the specific software release. The key element for the check is the Extension value.

Criteria: If a file type is not defined, this is not a Finding.
a) If the Confirm open after download option is not enabled for each file type, then this is a Finding.
b) If the Always show extension option is not enabled for each file type, then this is a Finding.

*Note: this check does not apply to Windows Vista

Fix Text: For each of the filetypes in question, verify the Confirm after download option and the always show extension option are checked.